REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of October 24, 2006 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. Nonetheless, the Examiner is expressly authorized to charge any deficiencies to Deposit Account No. 50-0951.

In the Office Action, Claims 1-24 were rejected under 35 U.S.C. 102(e) as being unpatentable over U.S. Published Patent Application No. 2004/0185842 to Spaur, *et al.* (hereinafter Spaur).

Applicants' Invention Predates Doyle

Applicants respectfully disagree that the Spaur teaches or suggests every feature recited in the claims. Applicants assert more fundamentally, however, that these issues are moot because Applicants' invention predates the January 28, 2003, effective date of Spaur.

Applicants conceived of their invention at least as early as September 19, 2002 and actively pursued its reduction to practice from a date prior to the effective date of Spaur. In support of their assertion, Applicants submit the Declarations attached hereto in accordance with 37 CFR § 1.131. The Declarations establish conception and continuing diligence from a time prior to the effective date of Doyle to the filing of the Application.

Along with the Declaration, Applicants also submit herewith a copy of Confidential Invention Disclosure No. BOC8-2002-0114, entitled *System and Method for Dynamic Data-Driven Privacy Protection and Data Sharing* (hereinafter Disclosure). The Disclosure, on November 4, 2002, was submitted by Applicants to an intellectual property (IP) professional employed by the assignee of Applicants' invention, International Business Machines Corporation (IBM). The Disclosure was insubstantially

modified on November 6, 2002. Indeed, as noted below, established IBM procedures for handling all such disclosures precludes any modification to the description of the invention itself once it has been submitted by an inventor. The Disclosure has not been revised subsequent to November 6, 2002.

The Disclosure explicitly describes and illustrates Applicants' invention. The written description and illustrations provided in the Disclosure are clear evidence of Applicants' conception of the claimed subject matter at least as early as September 19, 2002.

The Disclosure is an IBM confidential disclosure form. As such, it is a standardized document that, according to established IBM procedures, is used by IBM inventors to document the conception of an invention. Strictly-followed internal procedures established by IBM govern the use of all such confidential disclosure forms. One aspect of IBM's established procedures governing the use of such confidential disclosure forms is that no substantive modifications can be made to a confidential disclosure after it has been submitted to an IBM Attorney/IP Professional.

The written description, drawings, and each of the claims of the Application were prepared based upon the Applicants' attached Disclosure. Moreover, according to IBM's established procedures governing the use of such disclosures, the inventors reviewed the Application prior to its submission to the U.S. Patent and Trademark Office in order to ensure that the claims and written description contained therein were fully supported by the Disclosure.

Applicants exercised due diligence from prior to the effective date of Doyle to the date that the Application was filed. As expressly affirmed in the Declarations, Applicants from at least September 19, 2002, through the filing of the Application on June 24, 2003, worked diligently toward a constructive reduction to practice of the invention. Applicants initially worked with IBM's own in-house IP professionals during an internal

review of the invention, including assessing the invention in the context of related literature. Subsequently, Applicants worked with outside counsel retained by IBM to prepare and file the Application.

Outside counsel prepared the Application consistent with long-established professional practices, according to which cases are prepared on a first-in, first-out basis unless a particular application is associated with a bar date; those applications associated with dates are granted priority within the work queue. Outside counsel followed this professionally-accepted practice in preparing the Application in this case.

Evidence of Applicants' due diligence is submitted herewith in the form of various correspondences between Applicants, IBM IP professionals, and outside counsel. The correspondence evidences specific activity on specific dates relating to Applicants' pursuit of a constructive reduction to practice from a time prior to the effective date of Spaur.

The correspondence includes a letter of April 23, 2003, from an IBM professional to outside counsel instructing outside counsel to prepare a draft application for Applicants' invention. The correspondence also includes a letter of May 7, 2003, from outside counsel confirming receipt of those instructions. A draft application prepared by outside counsel was sent to Applicants on June 18, 2003, as evidenced by the e-mail from outside counsel on that date. Applicants reviewed the draft and provided their comments two days later, as evidenced by the inventors' e-mail to outside counsel on June 20, 2003. A final draft was also sent to Applicants, as evidenced by the email from outside counsel on June 20, 2003. Based upon the received comments and as evidenced by the receipt of the signed declaration and power of attorney dated June 23, 2003 from Applicants (filed on June 24, 2003), outside counsel filed the present Application.

Applicants respectfully submit that it was reasonable for them to rely on outside counsel in preparing the Application, and that outside counsel acted with diligence,

notwithstanding the constraints of other work obligations, in preparing the Application. Applicants further respectfully submit that the evidence of specific activity on specific dates clearly evinces Applicants prior conception and diligence in pursuing a reduction to practice from a time prior to the effective date of Spaur.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

AKERMAN SENTERFITT

Date: January 24, 2007

Gregory A. Nelson, Registration No. 30,577
Richard A. Hinson, Registration No. 47,652
Eduardo J. Quinones, Registration No. 58,575
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000

Disclosure BOC8-2002-0114

Prepared for and/or by an IBM Attorney - IBM Confidential

Created By Paul Moskowitz On 09/19/2002 01:34:38 PM EDT
Last Modified By George Salmi On 11/06/2002 04:08:42 PM EST

Required fields are marked with the asterisk (*) and must be filled in to complete the form .

***Title of disclosure (in English)**

System and Method for Dynamic Data-Driven Privacy Protection and Data Sharing

Summary

Status	Submitted
Final Deadline	
Final Deadline Reason	
*Processing Location	Boca Raton
*Functional Area	select [redacted]
Attorney/Patent Professional	[redacted]
IDT Team	select
Submitted Date	11/04/2002 04:53:14 PM EST
*Owning Division	select [redacted]
Incentive Program	
Lab	
*Technology Code	[redacted]
[redacted]	[redacted]

Inventors with a Blue Pages entry

Inventors: George Salmi/Raleigh/IBM, Moninder Singh/Watson/IBM@IBMUS, Paul Moskowitz/Watson/IBM, Xuan Liu/Watson/IBM@IBMUS, Sastry S Duri/Watson/IBM, Jung-Mu Tang/Watson/IBM, Jeff Elliott/Watson/IBM

Inventor Name	Inventor Serial	Div/Dept	Inventor Phone	Manager Name
> Salmi, George V.	[redacted]	[redacted]	[redacted]	[redacted]
Singh, Moninder				
Moskowitz, Paul A.				
Liu, Xuan				
Duri, Sastry S.				
Tang, Jung-Mu				
Elliott, Jeffrey G.				

> denotes primary contact

Inventors without a Blue Pages entry

IDT Selection

Attorney/Patent Professional
IDT Team
Response Due to IP&L

Richard Tomlin/Boca Raton/IBM

***Main Idea**

1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.

Problem:

Automotive telematics may be defined as the information-intensive applications that are being enabled for vehicles by a combination of telecommunications and computing technology. The automobile is, in effect, a computing platform to which mobile commerce services may be delivered. The services being delivered today on a regular basis and projected for the near future include navigation information, emergency roadside assistance, location-based services, delivery of digital information such as e-mail, entertainment, diagnostics and prognostics, and pay-for-use rental and insurance. These applications are enabled by the collection and use of data which may include information on the location of a vehicle as a function of time, emergency situations including accidents and personal health emergencies, diagnostic data on the many systems within the vehicle, services and entertainment that are selected by the vehicle occupants, the demographics of the driver and passengers, and the behavior of the vehicle driver.

Our framework protects the privacy and confidentiality of the data owners but also makes it possible for the data to be shared. The sharing of data enables a new business models in which services are developed based upon data derived from the vehicle. For example, real-time traffic analysis may be enabled by anonymized position and velocity data collected from a sample of vehicles on the road. Automotive manufacturers may use the feedback of diagnostic data associated with specific vehicle models to make improvements to a manufacturing line. Insurance companies may use a subset of the diagnostic and position data for improved risk analysis.

Privacy policies may be employed to protect privacy and confidentiality and to enable data sharing. In such systems, data is only released if the privacy constraints of the user can be met. Thus, an end-user can be confident that any entity collecting their personal data will not use the data in manner that is proscribed by the end-user. Such a system is described in U.S. Patent Application No. _____, filed on 11/7/2001, docket number YOR9-2001-0749, entitled System, Method, and Business Methods for Enforcing Privacy Preferences on Personal-Data Exchanges Across a Network. Unfortunately, the efficacy of such privacy policy matching systems is completely dependent on the integrity of the people and organizations that provide the services, or otherwise have access to the data. It is possible to create systems for the enforcement of privacy policies. Such systems are described in US Patent Application No._____, and No._____ both filed on 8/30/2002, dockets CHA9-2002-0008 and CHA9-2002-0006, both titled "SECURE SYSTEM AND METHOD FOR ENFORCEMENT OF PRIVACY POLICY AND PROTECTION OF CONFIDENTIALITY".

US 20030086520

However, none of the work cited addresses the problem of the dynamic nature of data of the kind that is derived from automotive telematics systems. The dynamic nature of the data, changing in space, time and with events means that policies based upon static information, e.g. name, address, social security number, income, etc. now have limited utility.

It is necessary to find dynamic policies that are based on temporal or spatial constraints or on events within the telematics domain. Examples and further explanation are provided below.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?

Solution:

Others have looked at the problem of mobile devices with respect to the context of the data requester or data subject. However, none look at data in a truly dynamic manner, changing policies dynamically as the data changes. The data we consider is dynamic. Though there is ongoing work in defining constraints based on properties for which the values are not known (at the time of writing the policy) but is known at the time of evaluating the policy, the underlying assumption still is that the value, albeit unknown, is static. Moreover, this assumes that constraints are specified over the values of certain properties; however, our event constraints do not make any such assumption...a constraint could be defined over an externally sensed and triggered event. See section 3 for references. Also, at the end of this section, we suggest a sample method claim that expresses the dynamic nature of our data and its relationship to privacy policies.

The solution to the problem is a new type of policy that deals with and may depend upon the dynamic data. For example, a spatial policy may be one that whose constraints allow release of data within NY and not outside NY, a temporal policy may require that data may be released only between 9 am and 5 pm. and an event policy may require that data be released if an airbag deployment event occurs and not otherwise. This in itself is novel. Examples of spatial. temporal and event policies are illustrated by the following scenario:

Example 1. Delivery Fleet Scenario:

The Jkl Trucking Company has a fleet of hundreds of delivery trucks. The company contracts for both long-distance and local pickup and delivery. Each truck is equipped with an in-vehicle computing device which monitors and transmits data periodically and upon request to the TSP Telematics Service Provider Inc. The dataset consists of identification information, such as vehicle and driver ID, time-stamped location data derived from GPS sensors, and diagnostic information derived from the vehicle bus, speed, fuel level, coolant temperature, etc., and a list of the cargo carried by the truck will be added for the shipment scenario.

There are a set of data protection policies in place at the TSP which determine which entities may view subsets of the dataset. These policies form a matrix for the modes of operation (applications) and entities (application service providers) that have access to the data from the Jkl trucks. For example, the matrix may look like Table 1.

Entity / Mode	1. Fleet Manager	2. Assistance Provider	3. LBS Service Provider	4. Receiver of Shipment	5. Traffic Analyst	6. Insu Com
Fleet Monitoring	All Data for all trucks	ID, Diagnostics	none	Exact Loc. (only trucks with shipments)	Exact Loc, (only inside analy. area) Anonym. ID	Diag Ano
LBS (gas, food, lodging, navigation)	Subset, e.g gas	none	ID, Exact or Fuzzy Loc. eg. zip code	none	none	non
Roadside Assistance	All	ID, Exact Loc, Diag, (only trucks req. asst.)	none	none	none	non

Additional modes and entities may enlarge the matrix. The sharing of data may be event based, or subject to geographic and temporal policies. For example, roadside assistance provider 1 may be limited to data from trucks in Connecticut while roadside assistance provider 2 to data from trucks in New York. Provider 2 may be further limited to access between the hours of 6:00 am and 5:00 pm.

For normal fleet monitoring the fleet manager may have access to all of the data from all of his trucks. The fleet manager's server at Jkl sends a request to the TSP for all the data from the Jkl fleet. At the TSP, policies are compared. The TSP in turn sends a request to the Jkl fleet for data from all of the Jkl trucks (or accesses the most recent dataset). The data is then sent to the fleet manager. The dataset from each truck contains a field showing whether a situation requiring roadside assistance exists for that truck (airbag has deployed, fuel tank is empty, or request by driver).

The data from the trucks is stored by the Jkl server. The fleet dispatcher may then display all of the positions of all the trucks in a given area, the state of Connecticut for example. Trucks needing assistance may be displayed separately or highlighted as part of the larger display.

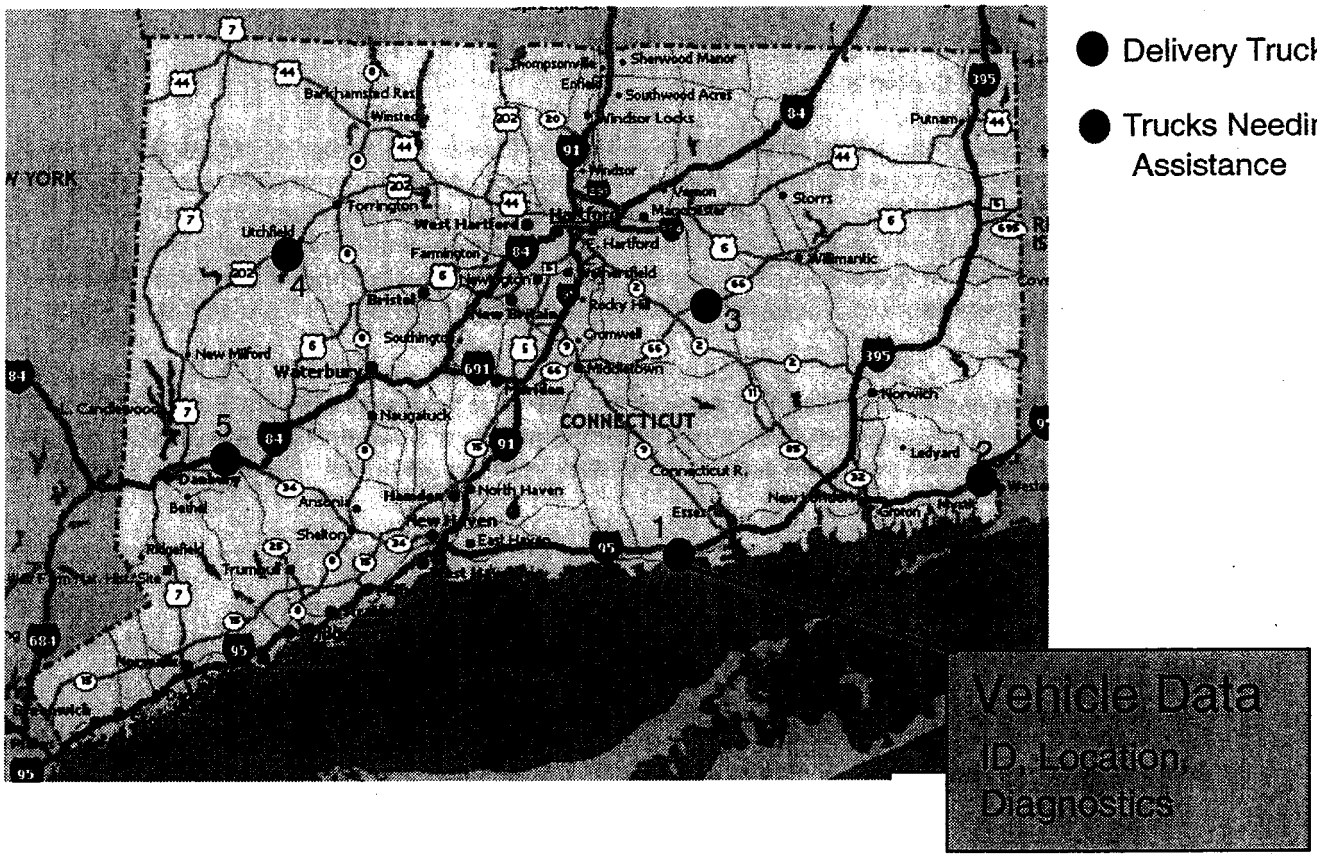


Figure 1 - Fleet Manager's Display (not all details of demo are shown)

Fleet manager View: Five trucks are shown. The images of the trucks, black dots with ID numbers, move along their routes, with periodic updates. By pressing the dot icon of a given truck, the complete data set can be shown. It will change in time.

Assistance Provider View: The Hjk Roadside Assistance Company in Connecticut has contracts to provide roadside service for the Jkl fleet of trucks. The server for Hjk receives a stream of ID and diagnostic data and requests for roadside assistance from Jkl trucks. Location data is not included until an assistance event takes place. However, there is a continuous flow of diagnostic data from all five the trucks.

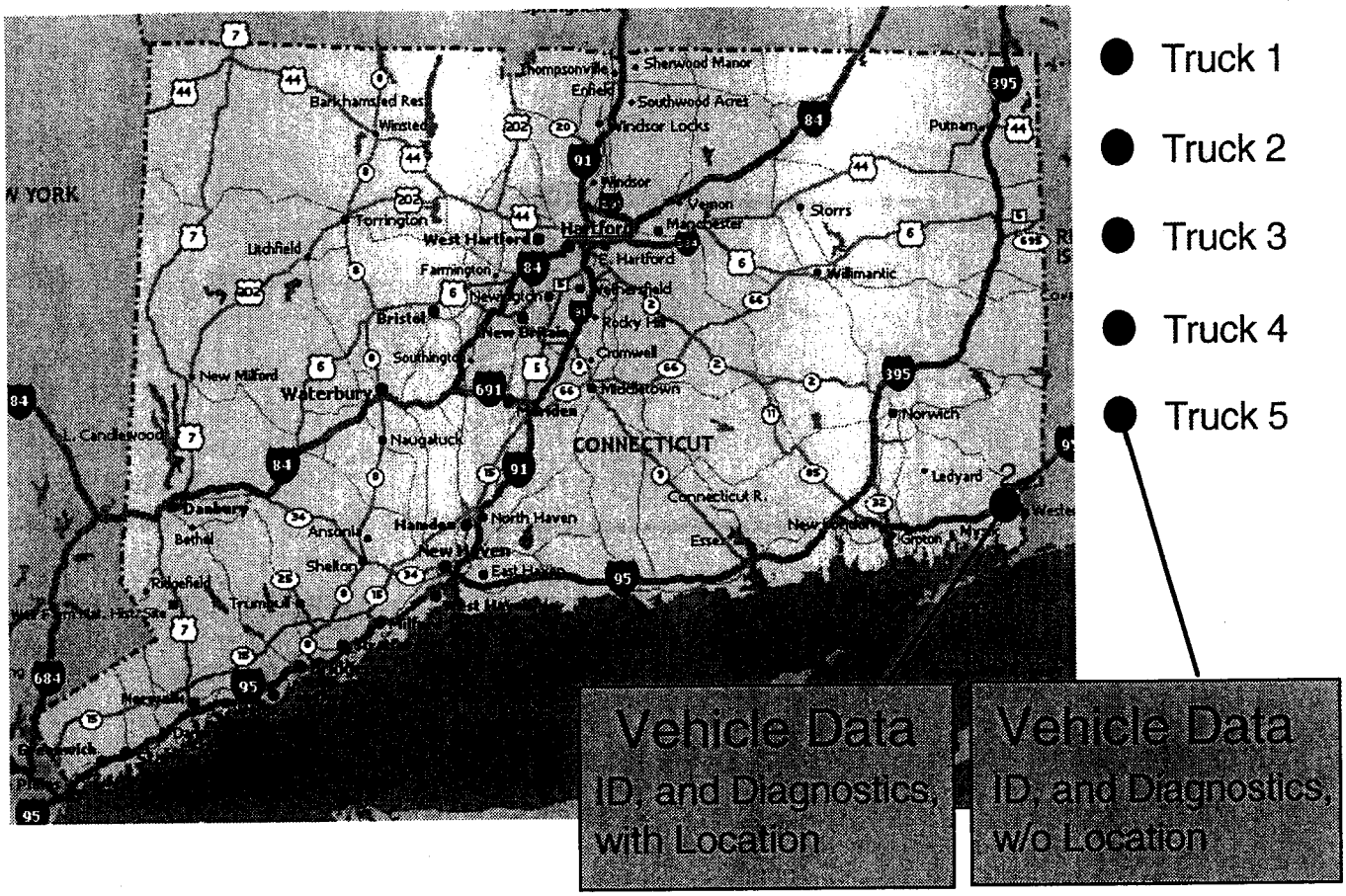


Figure 2 - Assistance Provider View

Diagnostic and ID data may be viewed for each of the five trucks by pressing the dot icon next to the map. Location data is not available until an assistance event occurs. The data for each truck will be updated automatically in the same way that the data that the fleet manager can view is updated.

Example 2. Vehicles in a Rental Fleet:

Fleet Managers have an interest in knowledge of locations and positions of vehicles. They would like to enforce contracted geographic boundaries, prevent or charge for misuse of vehicles, and track stolen vehicles

Renters of Vehicles have an interest in protecting privacy. They would like to use location-dependant services: navigation, hotel reservations, etc.
They will give up privacy in return for emergency assistance

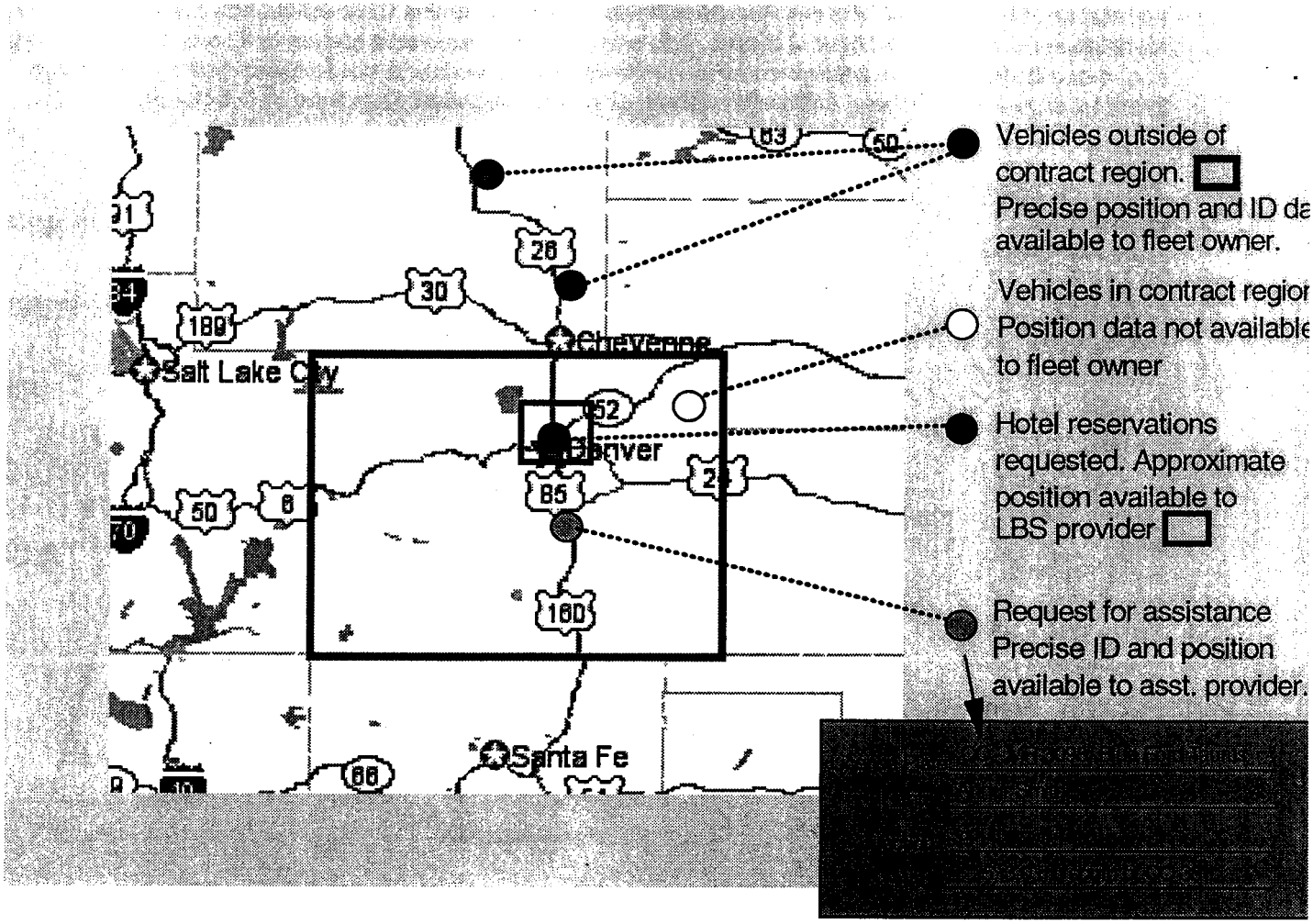


Figure 3. Rental Fleet Example - Fleet Manager View - Vehicles inside contracted region (outlined in red) are anonymous. Vehicles requesting reservation services are locatable within a local region, (outlined in blue). Vehicles outside of contracted region or vehicles requesting assistance have complete ID and position data available. Information from rental vehicles is filtered as privacy policies vary for specific services and
geographic areas. In this application, location information is not shown for normal operation inside of the contract area.

* * *

In addition to spatial, temporal and event policies, there are other solutions to dealing with dynamic data that others have not considered.

1. New types of the policies:
    a. Data constraint policies

Here, constraints restrict the data that can be released. In the existing referenced privacy systems as well as in other systems, data is partitioned orthogonally into the release/do-not-release sets by just picking (sets) of properties. e.g. release my diagnostic information, don't release GPS coordinates, release my VIN number, etc

We require constraints that can restrict the data in a more general form, i.e. policies that are defined by specifying constraints on the values of the data itself.

The two examples below illustrate this case:

i. Consider a policy that says that only data for the past 30 days can be released. Or only the last set of data recorded can be released.

While on the surface it may look like a temporal constraint, it is different since we are imposing a constraint on the data itself, thereby defining the data that can even be considered for release in the first place; not just defining temporal conditions under which the data can be released

ii. Consider another policy about personal data that says that phone numbers of area code 914 can be released but not phone numbers of 860 area code.

b. Situational policies

Consider policies that are based on various situations. For example

i. Consider a policy that states that data can be released only as long as the odometer is changing. Thus, data is to be released only while the vehicle is moving (to enable pay per use insurance) and not while it is parked.

Proposed solution: We allow policies to be specified at least using some simple constraints on data (using logical and arithmetic operators), this is especially useful for situational policies.

2. Resolving Policy Conflicts

In the referenced privacy system, it is assumed that all the constraints imposed by a policy should be satisfied for a data item to be released. So, even if one piece of the policy did not match the user's policy, the data would not be released even though the other parts of the policy match.

However, when we go to more complex policies, such a simple approach is just not sufficient.

For example,

1. Consider an event policy that says that GPS (location) data should be released if an airbag deployment event occurs

Consider a spatial policy that says that the GPS data should be released only if the vehicle is within NY

What happens when the airbag deployment event occurs in CT? Do we release data or not?

Again, one might say that event-based policies should have priority over location-based policies. However, that is too simplistic.

Consider the same policy as above with a slight change

2. Consider an event policy that says that GPS data should be released if oil level goes below 20%

Consider a spatial policy that says that the GPS data should be released only if the vehicle is within NY

In this case, one can actually argue that the privacy issues of the spatial policy are more important than the event policy since the event is not a critical one.

Proposed solution: These types of policies will be very likely in any real application/scenario and we must resolve conflicts. The way to do this is as follows:

a. Allow users to prioritize (absolutely or relatively) policies, either on an individual or group level as well as instance (specific event policy) and class level (all event policies)

Thus, a user could say that event based policies take precedence over spatial policies; or that airbag deployment events take precedence over spatial policies, but spatial policies take precedence over other event policies.

b. Allow users to specify whether a particular constraint is a hard constraint or a soft constraint. That would enable certain conflicts to be resolved easily. For example, an airbag event constraint may be a hard constraint (always needs to be satisfied) but a location constraint could be a soft constraint (that is, it could be violated in a conflict). That would allow the gps data to be released if an airbag deploys outside NY as in example 1 above.

c. Provide some sort of default structure that would be reasonable in most conditions.

3. Complex policies

So far, we have just talked about policies that are simple, based on values of a single property (although event based policies could be based on events that are triggered by multiple properties, but that leads to the need of being able to specify user-defined events). However, many real-life situations will demand more complex policies, that are sometimes binary or ternary constraints.

For example,

i. Consider a policy that states that location data should be released only if fuel level drops below 10% and the vehicle is in the middle of the Arizona desert (or outside NYC or out in the heartlands of some mid-west state etc)

Proposed solution: Similar to that suggested for (1). Allow users to create more complex policies by combining simpler policies using simple operators.

Example of Method Claims:

1. A method comprising:
examining the elements a first data set received from a subject
examining the elements of a second data set received from a subject
receiving a first request from an application for data elements of the first data set
assuring that the application requesting data has a privacy policy that complies with a first privacy policy of a privacy engine
and
receiving a second request from an application for data elements of the second data set
comparing the data elements of the first data set with the data elements of the second data set
determining from the comparison that the privacy policy of the privacy engine is a second privacy policy
assuring that the application requesting data has a privacy policy that complies with the second privacy policy of the privacy engine

2. The method of claim 1 where the data elements compared comprise location information (spatial or geofencing)

3. The method of claim 1 where the data elements compared comprise time information (temporal)

4. The method of claim 1 where the data elements compared comprise diagnostic information (event)

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?
See explanation and references in above sections 1 and 2.

Additional References,

The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002,

http://www.w3.org/TR/2002/REC-P3P-20020416/

A P3P Preference Exchange Language 1.0 (APPEL1.0), W3C Working Draft 15 April 2002, http://www.w3.org/TR/2002/WD-P3P-preferences-20020415

OASIS eXtensible Access Control Markup Language (XACML), 19 Mar 2002, http://www.oasis-open.org/committees/xacml/docs/

Instance-level access control for business-to-business electronic commerce, IBM Systems Journal, vol 41, no 2, 2002, Goodwin et al..

Individualized Privacy Based Access Control, Submitted to ACM Workshop on Privacy, Nov. 2002, Bohrer et al.

Concepts for Personal Privacy Policies, EC'01, Tampa, Florida, October 14-17, 2001, Einar Snekkenes.

Framework for Security and Privacy in Automotive Telematics, WMC'02 (Mobicom Workshop), September 28, 2002, Atlanta Georgia, Sastry Duri et al.

Microsoft Inc., A platform for user-centric application, http://www.microsoft.com/myservices/

AT&T, Privacy Minder, http://www.research.att.com/projects/p3p/pm

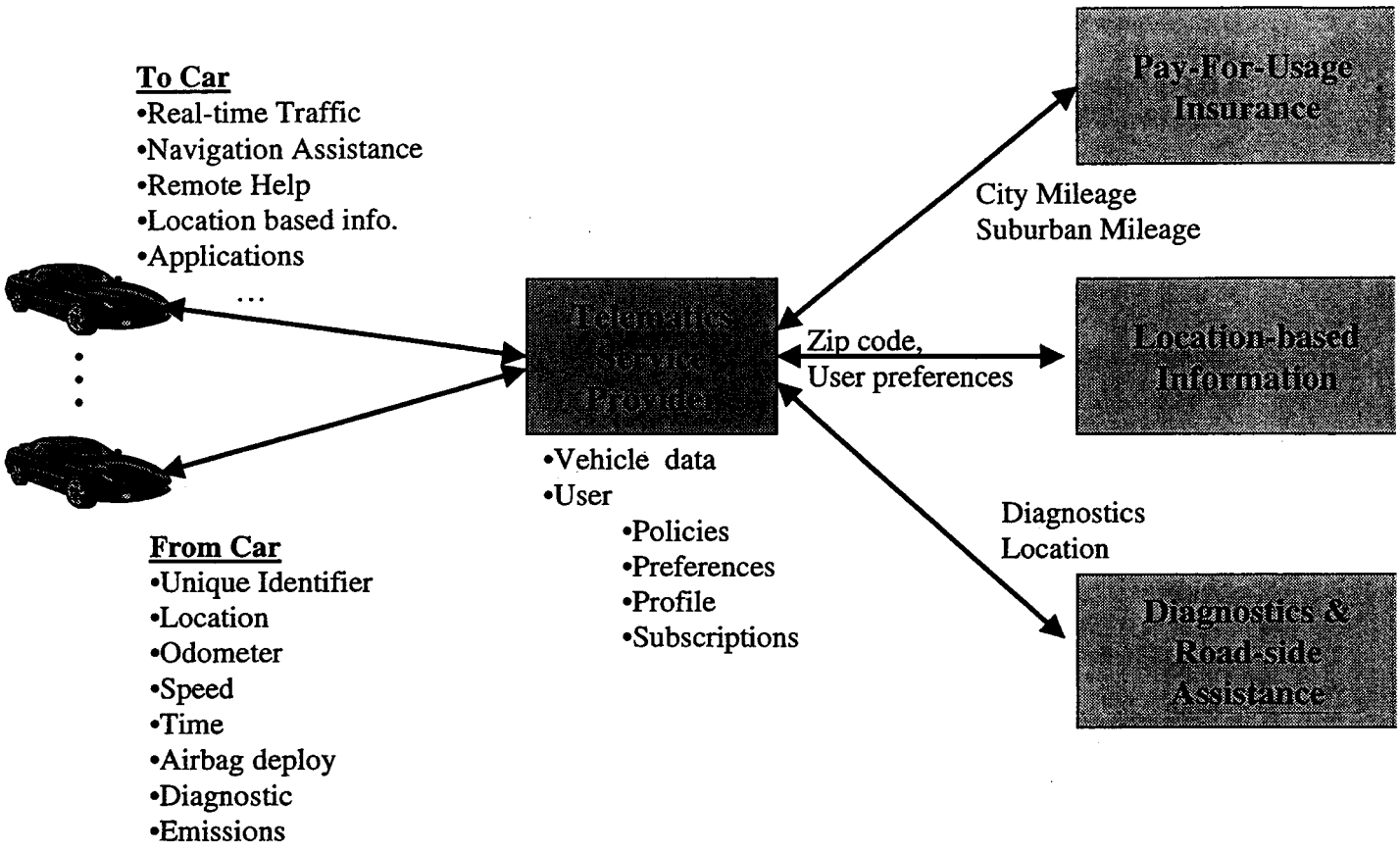
CPExchange, Global standards for privacy-enabled customer data exchange, http://www.cpexchange.org/standard/

BM, Enterprise Privacy Architecture (EPA), http://www.ibm.com/services/security/epa.html

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.
Implementation:

The system has been implemented in our laboratory. We plan to begin work to implement the solution for an IBM customer in 3Q2002.

The following diagrams illustrate the architecture and implementation of the solution.

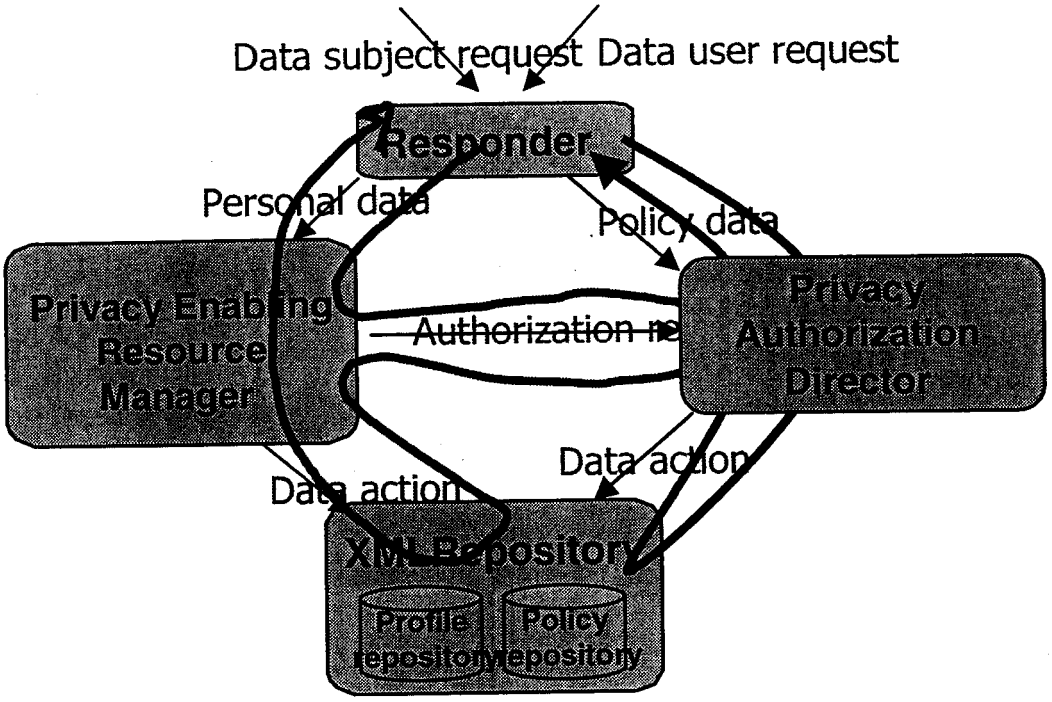


Data Flow in Telematics Applications

The Figure above shows an overview of a typical automotive telematics application. Cars shown in the picture are equipped with a wireless communication device, variety of sensors, and a car computer that has a display, sufficient memory, storage, and processing to run complex embedded applications and middleware. The car computer interfaces to car bus and other car sensors, for example, Global Positioning System (GPS) sensor, and collects car engine performance data, safety information, and car location.

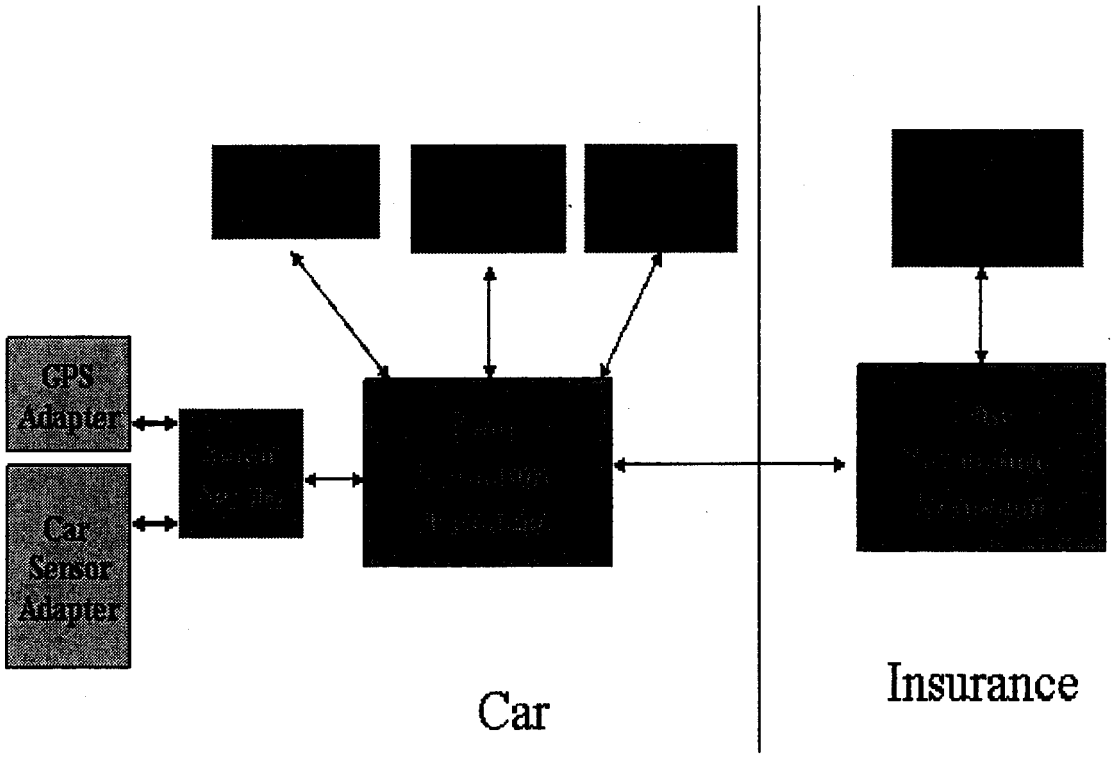
Car users subscribe to a telematics service provider (TSP) to get variety of services from application service providers (ASP) which include Pay-for-Use Insurance, Location-based Information, and Assistance as shown in Figure 1. In order to get services from a ASP, a car user needs to send some or all the information collected by the car computer to the ASP. In the setup shown above each car transmits data as necessary to telematics service provider which then provides data to different ASPs as needed. In this case, the telematics service provider acts as a service aggregation and a data broker. In addition to the data transmitted by cars the TSP stores user preferences and user subscriptions to services.

As shown in the figure different ASPs need different user data and use it for different purposes. The Pay-for-Use Insurance ASP needs user identification data, GPS data, miles driven to compute premiums and perform risk analysis. The Information ASP needs user location, and user preferences to send back information on local attractions. The data identifying user need not be sent to this service provider. The Road-side Assistance ASP needs car engine performance and safety information on regular basis, and car location in case of emergency.



Request Flow in Privacy Services

The above diagram shows high-level view of privacy services architecture and associated request flows. Typically, the privacy system receives two types of requests: (1) First type request flow, shown in blue, originates from a data subject creates policies to be applied while sharing data owned by the owner. The second type of request flow, shown, in red originates from a data user who requests data about a data owner from the privacy system. As shown, the responder receives requests. For the policy creating requests, it sends associated policy data to privacy authorization director (PAD). The PAD after verifying that the requestor, that is the data subject, has proper credentials creates requested policy. For the data user request, shown in red, the responder forwards the request to privacy enabling resource manager (PERM). The PERM first obtains authorization from PAD, then goes to the XML repository to obtain authorized data to return to the data user. The data user request flow can also be arranged such that the PERM first obtains all data from XML repository, and submits the data to PAD for authorization. The PAD then deletes what ever data that the data user is not authorized to receive.

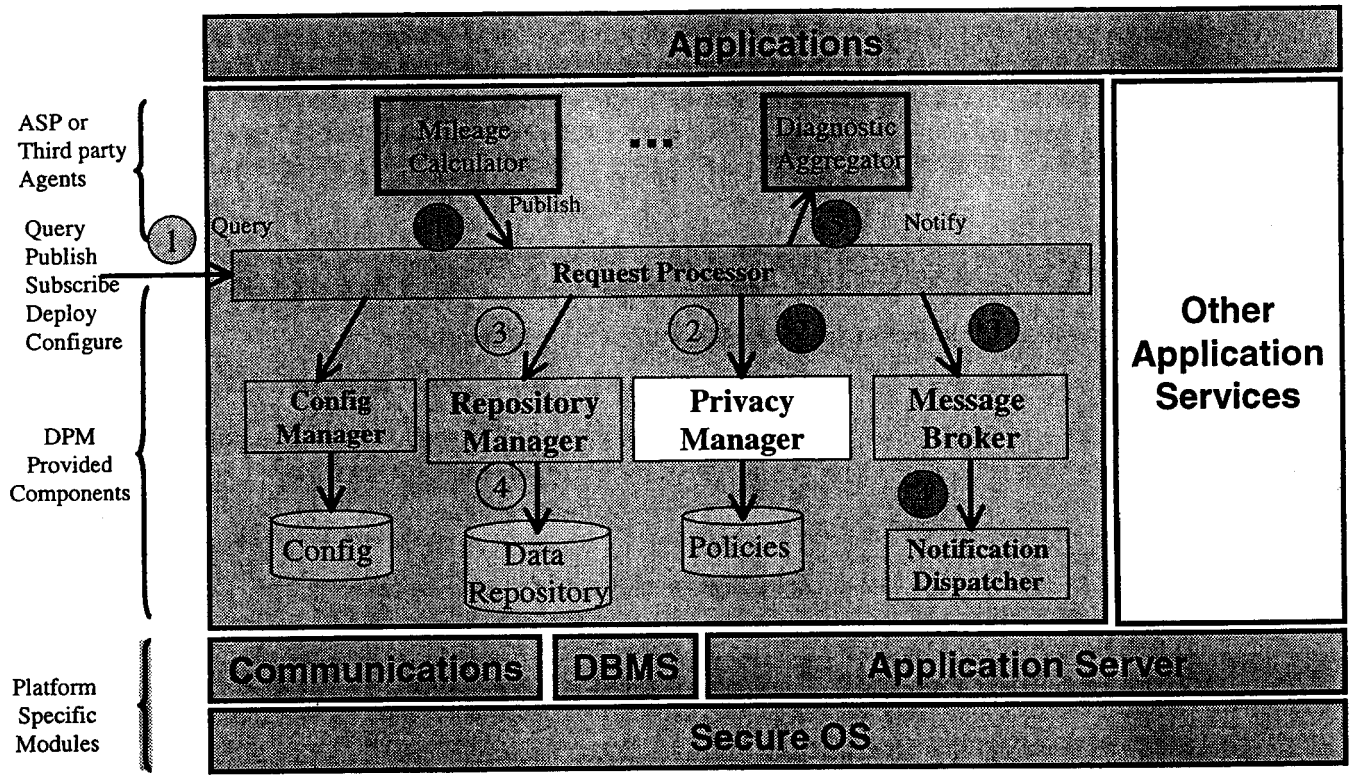


Implementation of Data Protection Manager in Vehicle

Applications follow the blackboard architectural style shown in the "implementation" figure for communicating with data sources, with other applications, and with external world. The Data Protection Manager provides an interface for information producers such as sensors or aggregation applications to publish data on the blackboard. Information consumers access this data through periodic queries or through a subscription/notification mechanism. We also extend the blackboard paradigm across the network. That is, applications at the TSP or ASP can submit queries to or receive notifications from the in-car blackboard mechanism.

The example illustrates how applications are composed in this framework. The GPS sensor in the vehicle periodically publishes location data items in the Data Protection Manager. The Classified Mileage Calculator can subscribe to the GPS data and compute with the help of a road map the total mileage driven on different types of roads. The results are again published in the Data Protection Manager. A Risk Analysis application running on the insurance server remotely subscribes to the aggregated and classified mileage data.

Blackboard-based architectures provide a simple paradigm for composing sensor-based applications. It is a common choice for building ubiquitous computing smart spaces, which depend on aggregated and interpreted sensor data. However, blackboards exhibit another key advantage for our privacy protection framework. Every data access passes through the central Data Protection Manager. This simplifies verifying that data accesses comply with the privacy policies.



Details of Data Protection Architecture

The "Details" figure above shows the data protection platform architecture. This architecture can be instantiated in vehicle, in telematics service provider and in application service provider settings by choosing appropriate implementations of the two bottom layers. In a car environment, we expect a real-time operating system such as QNX, whereas the TSP and ASP will use server operating systems such as Linux. For application server, in-car environments typically use the OSGi-based (Open Services Gateway Initiative,http://www.osgi.org/) platforms while server provider platforms use a typical Web Application Server. The Platform Protection Manager, which is a part of OS, monitors the integrity of all system software including the Data Protection Manager and provides security functions such as verifying signatures on applications. The Communications layer handles encrypted, authenticated, and monitored network connections. For example, it supports protocols like SSL or IPSec. The DBMS layer provides basic storage capabilities for the Data Protection Manager.

The picture above shows the sequence of steps involved in a query request originating outside the container (annotated with yellow number steps), and the steps involved in a publish request (annotated with blue step numbers) originating from an agent, the mileage calculator, from within the container. For the example query request the sequence of steps is as follows: In the step 1 the request processor receives the request, authenticates the requestor, if necessary. In the step 2, the request processor submits the request to privacy manager and obtains authorization for the requested data. In the step 3, the request processor submits the request along with authorization it obtained from privacy manager to the repository manager. In the step 4, the repository manager retrieves authorized data from data repository. In the step 5, (not shown in the picture) the repository manager returns the authorized data to request processor. In the step 6, (not shown in the picture) the request processor returns the query response back to the requestor.

For the example publish request shown the steps involved are as follows: In the step 1, the request

processor receives the request and authenticates the requestor if necessary. In the step 2, the request processor submits the request to privacy manager to obtain authorization for the publish request. In the step 3, the request processor submits the publish request along with the authorization it obtained from the privacy manager to the message broker. In the step 4, the message broker submits a message notification to the notification dispatcher. The the step 5 shows a subscriber to the published message is being notified.

***Critical Questions (Questions 1-9 must be answered in English)**

***Question 1**

[redacted]

***Question 2**

[redacted]

***Question 3**

[redacted]

***Question 4**

[redacted]

***Question 5**

[redacted]

***Question 6**

[redacted]

***Question 7**

[redacted]

***Question 8**

[redacted]

***Question 9**

[redacted]

Question 10

[redacted]

[redacted]

Question 11

[redacted]

[redacted]

***Question 1:** [redacted]

***Question 1** [redacted]

***Question 2:** [redacted]

***Question 3:** [redacted]

***Question 1:** [redacted]

[redacted]

*Question 1: [redacted]

[redacted]

*Question 2: [redacted]

[redacted]

[redacted]

*Question 1: [redacted]

[redacted]

*Question 2: [redacted]

[redacted]

*Question 3: [redacted]

[redacted]

*Question 4: [redacted]

[redacted]

[redacted]

Form Revised 09/01/02)

8051 Congress Avenue
Boca Raton, FL 33487

6169-408

April 29, 2003

Akerman, Senterfitt
222 Lakeview Avenue
Suite 400
West Palm Beach, FL 33401

REF: Invention Disclosure: BOC8-2002-0114
Title: **System and Method for Dynamic Data-Driven Privacy Protection and Data Sharing**
IBM Docket: BOC9-2003-0039

Dear Kevin,

Please prepare and file the above referenced case with the U.S. Patent and Trademark Office. A copy of the invention disclosure, patentability search results and inventor's comments are enclosed for your use in preparation of the application in accordance with IBM's format.

Sincerely,

[redacted]

Enclosures

Akerman Senterfitt
ATTORNEYS AT LAW

Boca Raton
Fort Lauderdale
Jacksonville
Miami
Orlando
Tallahassee
Tampa
West Palm Beach

222 Lakeview Avenue
4th Floor
West Palm Beach, Florida 33401-6147

Post Office Box 3188 *mail*
West Palm Beach, Florida 33402-3188

www.akerman.com

561 653 5000 *tel* 561 659 6313 *fax*

Direct Dial: 561-671-3658
E-Mail: kcuenot@akerman.com

May 7, 2003

[redacted]
IBM Corporation
8051 Congress Avenue
IMAD 4041
Boca Raton, FL 33487

RE: New U.S. Patent Application
SYSTEM AND METHOD FOR DYNAMIC DATA-DRIVEN PRIVACY PROTECTION AND DATA SHARING
IBM Docket No. BOC9-2003-0039; Our Reference No.: 6169-408

Dear [redacted]

Thank you for your letter dated April 29, 2003. In accordance with IBM standard protocol, a patent application will be prepared and filed in the above-referenced matter on or before October 26, 2003. We have requested additional information regarding a previous disclosure and may need to revise the due date of the application once the information is received. Notwithstanding, we will strive to prepare the patent application in an expedient manner.

As always, thank you for allowing us to be of assistance to you.

Very truly yours,

AKERMAN SENTERFITT

Kevin T. Cuenot

KTC/aa

Valee Bartels - IBM Docket BOC9-2003-0039; ASE Docket 6169-408

From: Valee Bartels
To: jge@us.ibm.com; jmtang@us.ibm.com; moninder@us.ibm.com; mosk@us.ibm.com; salmi@us.ibm.com; sastry@us.ibm.com; xuanliu@us.ibm.com
Date: 6/18/03 2:33 PM
Subject: IBM Docket BOC9-2003-0039; ASE Docket 6169-408
CC: Cuenot, Kevin T.; [redacted]

Re: Draft Patent Application for
SYSTEM AND METHOD FOR DYNAMIC DATA-DRIVEN PRIVACY PROTECTION AND DATA SHARING
IBM Docket BOC9-2003-0039; ASE Docket 6169-408

Dear Inventors:

Attached please find a draft of a patent application and associated drawings for your review in the above-identified matter. Please review the application carefully to ensure that the description of the invention accurately recites all of the invention's characteristics in the broadest possible manner, while also explaining, in detail, the preferred embodiment of the invention. The drawings should also be reviewed to confirm that they accurately depict the various details of the invention as you and your co-inventors understand them.

Importantly, please ensure that each inventor named on the cover sheet of the patent application has contributed to the conception of your invention as described in at least one of the claims. If for some reason we have neglected to list an inventor who has contributed to the conception of subject matter described in a claim, please so advise us immediately.

Once you have reviewed the application, please forward your comments and any suggestions you may have to us. We ask, however, that you coordinate your comments with one another and provide them to us through a single representative so that we may more effectively address each of your concerns and/or questions. Also, please be reminded that this application must be filed on or before June 24, 2003. We look forward to your comments.

Very truly yours,

AKERMAN SENTERFITT

Kevin T. Cuenot, Esquire*
Akerman Senterfitt
222 Lakeview Avenue, Suite 400
West Palm Beach, FL 33402-3188
Voice: (561) 671-3658
Fax.: (561) 659-6313
E-mail: kcuenot@akerman.com
Web: www.akerman.com
*Licensed to Practice Before the United States Patent and Trademark Office

Sent on Mr. Cuenot's behalf to avoid delay.

Valee Bartels
Legal Assistant to Kevin T. Cuenot
Akerman, Senterfitt & Eidson, P.A.
222 Lakeview Avenue, Suite 400
West Palm Beach, FL 33401

Ph: 561.653.5000, ext. 3434
Fax: 561.659.6313
E-mail: vbartels@akerman.com
Web: www.akermanIP.com

Valee Bartels - Re: IBM Docket BOC9-2003-0039; ASE Docket 6169-408

From: "Paul Moskowitz" <mosk@us.ibm.com>
To: "Valee Bartels" <VBartels@Akerman.com>
Date: 6/20/03 12:21 PM
Subject: Re: IBM Docket BOC9-2003-0039; ASE Docket 6169-408
CC: [redacted] "George Salmi" <salmi@us.ibm.com>, "Jeff Elliott" <jge@us.ibm.com>, "Jung-Mu Tang" <jmtang@us.ibm.com>, "Kevin T. Cuenot" <KCuenot@Akerman.com>, "Moninder Singh" <moninder@us.ibm.com>, "Sastry S Duri" <sastry@us.ibm.com>, "Xuan Liu" <xuanliu@us.ibm.com>

Kevin,

We have a few corrections and additions to make to the application. Please e-mail the updated application and filing papers. We can fax them back. I believe that notarization is not required.

Two of the figures have been modified. They are attached.

(See attached file: 6169-408 Figs3-4corrected.sdr)(See attached file: 6169-408 Fig7corrected.sdr)

Jeff's name should be spelled with two t's. · Elliott · Please correct the title page and any documents for filing.

Here are corrections, additions ·

1. Fig. 2 not a high-level architecture for tsp, but it is a high-level architecture for data protection manager
2. page 13, first line as it is now: â€œeach agent can be configured to access only needed informationâ€□ change it to â€œeach agent can be configured to access needed information as per their privacy policiesâ€□
3. paragraph 0053: the sentence as it is now: â€œthe system 400 can be implemented in a centralized environment â€¦ â€œ change it to read as follows: The system 400 can be implemented in TSP environment, in an ASP environment, and in a vehicle computing environment with appropriate choices for operating system, database, application execution environment, and security and communication protocols among other things.
4. configuration manager ;paragraph 58
5. Paragraph 0056: replace paragraph 0056 with the following: The agents 405 and 415 are deployed by ASP or TSP. Agents are signed by trusted third parties, and their signature is verified at the deployment time. The privacy policy accompanying agents states what private data they need to access and what computed data they are allowed to send back. All communication between agents and the ASPs is mediated by the data protection manager to prevent agents disclosing sensitive data they got access to. The agents can use this data to do their calculations, and can send back only the results of the calculations, but they cannot send the private data used in the calculations.

6. paragraph 0057:
o remove first sentence from the paragraph.
o Join the rest of the paragraph to the end of paragraph 0059.
7. paragraph 0059: replace the first sentence with the following: In operation all requests are received by the request processor 425 from application service providers 405, 410 and 490.
8. paragraph 0058: last sentence: change it to read: the notification dispatcher 465 can generate notifications to be posted to the request processor 425 which can then be forwarded to subscribers.

0013: line3 change to :

The privacy policy can specify constraint-based rules such as temporal rules, location rules,
event-based rules for sharing the telematics data under certain conditions.

Delete "Accordingly, the telematics data also can be compared with privacy policy."(not sure what this means)

0015: changed to :

A privacy manager can be included that is configured to compare the privacy policy
specified by the received requests of telematics data with the privacy policy information
associated with the requested telematics data.

Each agent can be configured to access telematics data on behalf of that application service
provider.

0010
Telematics data can include, but is not limited to, vehicle diagnostic information, vehicle location information, temporal information, vehicle trajectory and vehicle acceleration and deceleration information,
..additionally Telematics data can also include the position, status and biometrics of the driver and passengers

Please add additional terms to claim 4 and other similiar dependant claims.

0082 Change first sentence to read -

In any case ... provided to to the requester as specified by the privacy policy. Delete everything from "ASP" to end of pararagraph.

Thanks, -Paul

Paul Moskowitz, Ph.D., P.E.
Research Staff Member
IBM Watson Research Center - Hawthorne, NY
Internal Tieline: 863-7156, fax: 863-6001
External Phone: 914-784-7156, fax: 784-6001

"Valee Bartels" <VBartels@Akerman.com>
06/18/2003 02:40 PM

To: Jeff Elliott/Watson/IBM@IBMUS, Jung-Mu Tang/Watson/IBM@IBMUS, Moninder Singh/Watson/IBM@IBMUS, Paul Moskowitz/Watson/IBM@IBMUS, George Salmi/Raleigh/IBM@IBMUS, Sastry S Duri/Watson/IBM@IBMUS, Xuan Liu/Watson/IBM@IBMUS
cc: "Kevin T. Cuenot" <KCuenot@Akerman.com>, [redacted]
[redacted]
Subject: IBM Docket BOC9-2003-0039; ASE Docket 6169-408

Re: Draft Patent Application for
SYSTEM AND METHOD FOR DYNAMIC DATA-DRIVEN PRIVACY PROTECTION AND DATA SHARING
IBM Docket BOC9-2003-0039; ASE Docket 6169-408

Dear Inventors:

Please be advised the password remains "mayday".

Very truly yours,

Valee Bartels
Legal Assistant to Kevin T. Cuenot
Akerman, Senterfitt & Eidson, P.A.
222 Lakeview Avenue, Suite 400
West Palm Beach, FL 33401
Ph: 561.653.5000, ext. 3434
Fax: 561.659.6313
E-mail: vbartels@akerman.com
Web: www.akermanIP.com

From: Kevin T. Cuenot
To: jge@us.ibm.com; jmtang@us.ibm.com; moninder@us.ibm.com; mosk@us.ibm.com; salmi@us.ibm.com; sastry@us.ibm.com; xuanliu@us.ibm.com
Date: 6/20/03 5:47PM
Subject: IBM Docket No. BOC9-2003-0039; Our Docket No. 6169-408

RE: Final Draft Patent Application for
METHOD, SYSTEM, AND APPARATUS FOR DYNAMIC DATA-DRIVEN PRIVACY POLICY PROTECTION AND DATA SHARING
IBM Docket No. BOC9-2003-0039; Our Docket No. 6169-408

Dear Inventors:

Enclosed please find for execution a final draft of the above-identified patent application, the Declaration and Power of Attorney, the Assignment, the Oath and Assignment for the Republic of China, and a REDLINED version of the patent which evidences the changes you have requested and which have been incorporated into the final version as well as the drawings. A "clean" version of the patent application also has been included for your convenience.

After your review of the REDLINED patent application and drawings, if the patent application accurately recites all of the invention's characteristics, please print out the formal documents and have all of the inventors sign and date the enclosed documents where indicated.

Please note that pursuant to IBM's request, all of the signatures must be contained on the same documents Once the documents are fully executed, please send the documents to our office via facsimile copy for filing with the patent application. Please also send the original documents to us via regular mail.

Finally, if you feel we have not fully addressed your concerns, or have any questions, please do not hesitate to contact us prior to executing the documents.

Very truly yours,
Kevin Cuenot

Kevin T. Cuenot
Akerman Senterfitt
222 Lakeview Avenue, Suite 400
West Palm Beach, FL 33401
(561) 671-3658 (Phone)
(561) 659-6313 (Fax)
E-Mail: kcuenot@akerman.com

CC: Bartels, Valee; Buchheit, Brian; Venturelli, Elaine